Information Security Compliance Review
Office of Audits and Compliance
February 22, 2008

The Office of Audits and Compliance (OAC) Information Security Branch (ISB) conducted an Information Security Compliance Review of The Office of Audits and Compliance on February 22, 2008. The review covered 8 different areas. The Office of Audits and Compliance was fully compliant in 5 areas, partially compliant in 2 areas, and non-compliant in 1 area. The overall score is 91%. The chart below details these outcomes. Other observations are also noted.

FINDINGS SUMMARY:

		Score	Compliant	Partial Compliance	Non Compliant
STAFF COMPUTING ENVIRONMENT					
1.	Use Agreement (Form 1857) is on file.	100%	C		
2.	Annual Self-Certification of Information Security Awareness and Confidentiality forms are on file.	83%		PC	
3.	Information security training is current.	100%	C		
4.	Staff log on are using own password.	100%	C		
5.	Network access authorization is on file.	100%	C		
6.	Physical locations of CPUs agree to inventory records.	100%	C		
7.	Staff CPUs labeled “No Inmate Access.”	N/A	N/A	N/A	N/A
8.	Staff monitors are not visible to inmates.	N/A	N/A	N/A	N/A
9.	Anti virus updates are current.	86%		PC	
10.	Security patches are current.	57%			NC

INMATE COMPUTING ENVIRONMENT (Education, Library, Clerks)					
11.	Physical location of CPUs agrees to inventory records	N/A	N/A	N/A	N/A
12.	CPU labeled as inmate computer.	N/A	N/A	N/A	N/A
13.	Anti virus updates are current.	N/A	N/A	N/A	N/A
14.	Inmate monitors are visible to supervisor.	N/A	N/A	N/A	N/A
15.	Portable media is controlled.	N/A	N/A	N/A	N/A
16.	Telecommunications access is restricted.	N/A	N/A	N/A	N/A
17.	Operating system access is restricted.	N/A	N/A	N/A	N/A
18.	Printer access is restricted.	N/A	N/A	N/A	N/A

Total of Tests	5	2	1

Overall Percentage 91%

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of the Information Security Compliance Review were to:

- Assess compliance to selected information security requirements,
- Evaluate other conditions discovered during the course of fieldwork that may jeopardize the security of information assets of the facility or of the Department, and
- Provide information security training for management and staff.

The Information Security Branch (ISB) did not review any Prison Industry Authority computers.

In conducting the fieldwork the ISB performed the following procedures:

- Interviewed senior management, information technology staff, institutional staff, and computer users.
- Asked staff to provide evidence that all authorized computer users had Acceptable Use Agreement forms and appropriate training support documentation on file.
- Tested selected information security attributes of users and IT equipment using three different population samples. This included both the staff and inmate computing environments.
- Reviewed various laws, policies and procedures, and other criteria related to information security in the custody environment.
- Conducted physical inspection of selected computers.
- Observed the activities of the information technology support staff.
- Analyzed the information gathered through the above processes and formulated conclusions.

FINDINGS AND RECOMMENDATIONS

The ISB provided a copy of our review guide to your IT staff. It contains criteria and detailed methodology. That information, therefore, is not duplicated under each finding.

ISB's findings and recommendations are listed below. ISB staff discussed them with management in an exit conference following our fieldwork. Please contact us if you would like to discuss further any of these issues.

1. Self-certification of annual information security awareness and confidentiality is not on file for all computer users. (83% compliance)

All but one user had completed self-certification forms on file. It should be noted that the user had the form but it was missing the signature of their supervisor.

Recommendation: Require all computer users to self-certify their information security awareness and confidentiality agreement on an annual basis using form CDCR ISO-3025 or equivalent. (DOM 49020.10.1)

2. Staff computers did not have up-to-date antivirus software. (86% compliance)

All but one computer had up to date antivirus software installed on their computer. The user of the noncompliant computer was on vacation for a period exceeding the time limit tolerance for the test. Had the user logged on during that time, the antivirus files on the computer would have likely been up to date. The auditor performed a manual update to the computer with no problems.

Recommendation: Update antivirus software on all staff computers. (DOM 48010.9)

3. Staff computers did not have up-to-date security patches. (57% compliance)

Recommendation: Update security patches on all staff computers. (DOM 48010.9)

OTHER OBSERVATIONS:

Observation 1: Critical data in some areas is not being backed up.

Recommendation: Each department manager should identify all data that is critical to their operations, including locally developed databases, and develop back-up and restoration procedures. A back up schedule should be established and enforced. (DOM 48010.9.3)